Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Consolidated Developers Toolkit
Users Guide
(Solaris 2.5.1)

Version 3.0

January 3, 1997

Prepared for:

Defense Information Systems Agency

Updated by:

Defense Information Systems Agency
45335 Vintage Park Plaza
Sterling, VA. 20166-6701

Table of Contents

This page intentionally left blank.

1. Introduction

The Consolidated Developers Toolkit consists of tools which developers will require in order to develop applications for DII. Contained within this toolkit are the following:

- **!** DII_DEV - The segmentation tools for segmenting COTS, GOTS and applications for DII 3.0
- **!** SeComp - DII Security Compliance (SeComp) tool will provide functions and procedures to ensure that new COE kernel and application segments do not disrupt the DII recommended security configuration.
- **!** UBDEV - Unified Build Development

1.1 Installation Instructions, DII 3.0 Developer's Toolkit

1) This tape is a relative tar, and will place all items under a **TOOLS** subdirectory.

2) To install the toolkit, **login as root** and open an **xterm**.

3) Change to the directory that you would like **TOOLS** to reside under.

4) Enter the following command:

tar xvf /dev/rmt/*X*mn

where *X* is the number designating the tape drive in which you placed the tape.

Below are the directory trees that will be installed on your machine:

SUN

Solaris 2.5.1

./TOOLS

/DII_DEV

/Scripts
/bin
/data
/libs
/man
/example
/include
/SampleSegments

/secomp
/masters
/reports
/tasks
/tmp
/util

/UBDEV
/UB
/Printer

2. Segment Tools

2.1 Installation of Segmentation Tools and Environment

The MakeTOOLSEnv script sets up the environment variables for using the tools.

The command for running the script :

```
% source Scripts/MakeTOOLSEnv
```

Please note that in order for the MakeInstall tool to work correctly, it is necessary for the user to set an environment variable called TOOLS_HOME to where the TOOLS directory resides.

This environment variable will be set up by the script. At the prompt "Enter the tools home dir (default is /h/DII_DEV) >" enter the home directory or press RETURN to make TOOLS_HOME equal to /h/DII_DEV.

This will allow valid device information to be displayed when the user is prompted to enter a tape device.

The TestInstall and TestRemove tools must be run as root. It is recommended that VerifySeg and CalcSpace also be run as root, because they must write to files in the SegDescrip directory. If the user does not have write permission to the SegDescrip directory, then VerifySeg and CalcSpace will fail. If a user does not have root permission, then a root user should set the owner sticky bit for the Testinstall ,TestRemove, CalcSpace and VerifySeg tools so that the tools will run with an effective uid as root.

Man pages are provided for each of the segmentation tools and can be found in the “man” directory under the “DII_DEV” directory.

3. SeComp

The DII Security Compliance (SeComp) tool will provide functions and procedures to ensure that new COE kernel and application segments do not disrupt the DII recommended security configuration. The recommended security configuration is based on the DII Security Checklist that will provide the foundation criteria for certification and accreditation (C&A.) The SeComp tool will be updated as the DII Security Checklist and the C&A procedures are developed to completion.

The SeComp tool is currently capable of executing on both the Solaris and HP-UX platforms. The Solaris version is based on the Automated Security Enhancement Tool (ASET) modified for GCCS and DII. The compliance tools for the NT, IBM AIX, and other accepted DII platforms will be integrated into upcoming versions of the SeComp tool. COTS tools will be used to the extent that they are available, integratable, and can be made operational in the DII environment without undo stress to security compliance process.

The initial version of the SeComp will not be segmented. The platform dependent versions will be provided via tar formatted 8 millimeter tape for the Solaris and for the HP-UX. The reasoning for this is to allow the security analysts in the security compliance process to inject as much input as possible into to improvements or enhancements to the SeComp before finalizing the product. The author of the tool will be available for instruction and guidance.

3.1 SeComp Functional and Procedural Overview

The purpose of the security compliance tool (SeComp) is threefold:

- The SeComp will be used to *prepare* a COE suite to ensure that the COE suite is in the DII recommended security configuration at the beginning of a regression test operation.

- The SeComp will be used to ensure that the COE suite *remains* in the recommended security configuration at the end of a successful segment installation

- The SeComp will be used to ensure that the COE *remains* in the recommended security configuration at the end of a successful segment test execution.

The SeComp tool is accompanied by this set of SeComp procedures. The SeComp tool will provide a set of reports that will be analyzed to detect any modifications that a new COE kernel or application may have imposed on the DII recommended security configuration.

The SeComp reports will be examined by 2 teams of analysts, the security configuration team and the risk analysis team. The first team is identified within the Quality Assurance process. These

analysts will determine if the recommended security configuration has been affected, identify the specific discrepancies, and make recommendations concerning the importance of the discrepancies. The second team will be identified by the DII Security Management as the risk analysis team. This team of analysts will determine the risk factor based on the identified discrepancies and knowledge of the DII threat environment. The risk analysis team will determine whether or not the segment is acceptable given the discrepancies against the DII security configuration.

3.2 SeComp Quality Assurance Analysis

The SeComp tool will be inserted in the Quality Assurance (QA) phase at the Operational Support Facility (OSF), Sterling, Va. The QA team performs its mission using the most recent versions of the DII segments and therefore provides the most robust testing environment.

The QA security configuration analysts will execute the SeComp tool in the manner described. After each execution, the security configuration analyst will:

- Collect the SeComp reports
- Examine the SeComp reports for discrepancies with the DII security configuration
- Document the procedures performed and any discrepancies found.

The important piece of this effort is to document the findings on each segment. This information must be documented accurately. This information is then passed to the risk analysis team where the discrepancies are analyzed from a risk perspective.

3.3 SeComp Risk Analysis

The QA security analyst will forward the SeComp reports and the security analyst checklists to the risk analysis team. The risk analysis team will examine the QA findings and assess them regarding any discrepancies that may have been found. It is expected that most segments will comply with the security configuration, and in these cases, the risk analysis team will only need to confirm the QA findings.

It is recommended that segments should be approved for distribution only after the risk analysis team has indicated that the new segment been accepted and has included any statements regarding the conditions pertaining to the acceptance.

It is recommended that guidelines be established that bound the limits of what may be determined acceptable. For example, object permissions of security-related features at the operating system (OS) level should be considered untouchable. Further, objects that have been known to usurp root privilege if adequate protections are not maintained should be considered in a like manner.

It is recommended that the risk analysis team be delegated an appropriate level of authority to perform its mission. The level of authority should be sufficient to reject a segment on the basis that it would incur unreasonable risk to the security posture of the DII. The basis for these decisions should be documented and be required to reference the appropriate security policy and requirements statements. The documentation identifying the cause for rejection and the segment can then be returned to the vending source.

3.4 SeComp QA Procedure

The initial version of the SeComp tool will execute in the same manner as the ASET and SCCT security configuration tools. The SeComp has been streamlined to reduce output and will be further modified in this manner in the next version.

There is one step that must be completed manually by the security configuration analyst at the end of all three steps described in the next paragraphs. After the master reports are printed, the on-line reports must be deleted. This will ensure that each step generates a set of master reports for each execution of the SeComp tool. This step will be automated in the next version of the tool.

3.4.1 Configuring the COE Test Suite

The first step in the security compliance process is to ensure that the target COE suite used in the QA testing is in the recommended security configuration for the DII. This configuration is based on the DII security checklist and is incorporated in the programs that comprise the SeComp tool. The SeComp reports will identify specific areas that are out-of-compliance with the DII security checklist.

The QA security configuration team should strive to ensure that the QA systems are continuously maintained in this state of security by not overriding or otherwise manipulating the configuration. The applications submitted for approval in the DII COE MUST show themselves capable of operating within the boundaries of the DII security configuration. COE segments that modify the security configuration must be identified and reported.

Once SeComp has executed in this initial phase, the generated reports are analyzed. The SeComp will identify areas that are out-of-configuration with the recommended security configuration. Before continuing to install the application segment to be tested, the QA personnel MUST bring the system into configuration by modifying the out-of-configuration parameters. Once the out-of-configuration parameters have been brought into configuration, the SeComp should be executed against the specific report areas where the out-of-configuration parameters are tested. The reports should be re-analyzed to ensure compliance. Once the initial compliance is ensured, testing may begin for the COE segment.

3.4.2 Install and Test the Target COE Segment

The second step is to install the COE segment to be tested. It is imperative to follow the installation instructions verbatim during this process in order to identify specific problem areas.

After SeComp has executed in the installation phase, the generated reports are analyzed. The SeComp will identify areas that are out-of-configuration with the recommended security configuration. The security configuration analyst must document any out-of-configuration details that are identified in the SeComp report before continuing the analysis of the segment. After all out-of-configuration details have been documented, the analyst may proceed.

It is recommended that the security configuration analyst be allowed to reset the out-of-configuration parameters that were found at this point, before testing the COE segment functions. Once the out-of-configuration parameters have been brought into configuration, the functional testing may begin. This will determine if the functional performance of the segment is affected when operating in the DII recommended security configuration. The analyst must document any operations that appear to be inhibited or prevented because of the corrected out-of-configuration parameters.

It is also recommended that if the COE segment fails to operate because of the recommended DII security configuration, that the security configuration analyst be allowed to configure the parameters back to the values set by COE segment during the segment installation so that the segment can be functionally tested.

3.4.3 Examine the COE Test Suite Operational Configuration

The third step occurs after the COE segment has been functionally tested. It is imperative to follow the operational instructions verbatim during this process in order to identify specific problem areas.

After the COE segment has been tested, execute the SeComp tool again and analyze the reports generated. Once again, the SeComp reports will identify areas that are out-of-configuration with the recommended security configuration. The security configuration analyst must document any out-of-configuration details that are identified in the SeComp report before completing the analysis of the segment. After all out-of-configuration details have been documented, the analyst may proceed.

After the functional testing has been completed, the security configuration analyst must reset any out-of-configuration parameters that were found up to this point to ensure that the QA test suite is left in the recommended security configuration. Once the out-of-configuration parameters have been brought into configuration, the COE segment testing may be considered complete.

The final step in the QA process is to turn over all SeComp reports and accompanying documentation to the risk analysis team.

3.5 SeComp Functional Details

The SeComp tool must be installed in a protected hierarchy on the file system, for example, in `/etc`. This tool should not be generally accessible to the public to ensure its integrity during operation.

The SeComp tool operates with the same parameters as the ASET and SCCT tools, and will produce the following reports:

- Identification and Authentication (I&A) report
- Discretionary Access Control (DAC) report
- System Configuration (sys_config) report
- Audit report
- Password Vulnerability report
- World-Writable report
- Unknown UID report

These reports provide the configuration details of the system and will identify if there are any out-of-configuration details.

3.5.1 SeComp Options

The SeComp program supports 6 options:

- -c : initial configuration execution
- -t : segment install execution
- -o : segment operation execution
- -d : where the runtime directory is located

- -r : where the reports directory hierarchy is located
- -m : where the masters directory hierarchy is located.

These options allow total flexibility for the configuration of the SeComp program execution and collection depositories.

3.5.2 SeComp Operations

SeComp may be run on any server in the enterprise configuration and its reports may be collected on any server. Both may be located on different servers. The only considerations for the server should be space and performance. The SeComp runtime software and reports do not take up a great deal of memory, however it would be prudent to reserve at least 10 megabytes for its operation.

SeComp clients use the automount NFS features to connect with the SeComp server. This means less load on the network and only during the periods when SeComp is actually in operation. Once the SeComp software completes, the connections will be automatically disconnected.

3.5.3 SeComp Commands

There are four commands used with SeComp that reside in the SeComp runtime directory (e.g., `/etc/secomp`):

- run_secomp
- view_status
- view_rep
- view_allrep

The `run_secomp` script is a front end to the `secomp` shell script that should be used to execute the SeComp program. The configuration sections cover the details of this program later, however, there are no option to the command, to execute enter:

```
cd /etc/secomp
run_secomp
```

The `view_status` is a front-end to the task status checking script `~/secomp/util/taskstat` script. This program will print the status of the secomp program as found in the `~/secomp/reports/[`*`hostname`*`]/latest` report directory. This program will understand its environment and know where the reports directory is. To execute the program from the command line enter:

```
cd /etc/secomp
./status
```

The `view_rep` is a script that displays a given report for a given host name. This program will print the report for the named SeComp task as found in the `~/secomp/reports/[`*`hostname`*`]/latest` report directory with the suffix *.rpt*. This program will understand its environment and know where the reports directory is. This command does have two required arguments, first the report name in the format *task_name.rpt* and, second, *hostname* as it is defined in the system `/etc/host` name file for the host whose report is to be reviewed. To execute the program from the command line enter:

```
cd /etc/secomp
./view_rep cckpswd hostname
```

The `view_allrep` is a script that displays all of the reports found for a given host name. This program will print the reports for the SeComp tasks as found in the `~/secomp/reports/[hostname]/latest` report directory with the suffix *.rpt*. This program will understand its environment and know where the reports directory is. This command does have one required argument, the host name as defined in the system host name tables for the host whose report is to be reviewed. To execute the program from the command line enter:

```
cd /etc/secomp
./view_rep hostname
```

3.5.4 SeComp Tasks

The SeComp tool provides the following tasks:

- Identification and Authentication (I&A) task
- Discretionary Access Control (DAC) task
- System Configuration (sys_config) task
- Audit task
- Password Vulnerability task
- World-Writable task
- Unkown UID task

3.5.5 SeComp Configuration

The SeComp program will be configured at the time the SeComp segment is installed. There may be modifications to this configuration desired by the enterprise. If this is the case, the modifications must consider the environment the SeComp tool is to be operated in, most particularly, the client-server environment. The security manager must decide and plan:

- the server to be used as the SeComp server
- the locations of the SeComp repository directories (reports, archive, and masters)
- the SeComp tasks to be executed
- the automount configuration changes required at the clients
- the NFS file-share setup on the server.

The next sections outline the configuration details of the SeComp program and identify the default configuration settings that will be applied when the SeComp segment is installed.

3.5.5.1 SeComp Server and Standalone Configurations

The SeComp configuration consists of three primary decisions defining how the program will be run:

- where the SeComp runtime software will be located in the file system hierarchy of the server
- where the SeComp generated report hierarchy will reside
- which tasks the SeComp will execute.

All of these decisions will be installed in this recommended configuration:

- the SeComp runtime software will be installed to `/etc/secomp`
- the SeComp generated report hierarchy will reside in `/etc/secomp/reports`

3.5.5.2 SeComp Configuration Files

The SeComp configuration files are all located in the SeComp hierarchy and are:

```
~/secomp/secompenv
~/secomp/run_secomp
~/secomp/.secomp_paths
```

where the tilde represents the location of the SeComp hierarchy (defaults to `/etc`).

3.5.5.3 secompenv File

The `/secomp/secompenv` file contains most of the variable setting and exporting required for SeComp. The only variable that should be touched here is the default `TASK` settings. This variable controls the tasks to be executed if it has not been specified in the `/secomp/run_secomp` file.

3.5.5.4 run_secomp File

The `/secomp/run_secomp` file contains the SeComp startup instructions and command line. Additionally, the `TASKS` variable may be set here also; this is useful for the client configuration elements. The variables defined in this file will tell the SeComp program where the locations of the runtime software, reports, and master directories are shown next with their default settings:

- **!** `SECOMPPATH=/etc` - defines the location of the SeComp runtime software
- **!** `REPPATH=/etc` - defines the location of the SeComp reports directory
- **!** `MASTPATH=/etc` - defines the location of the SeComp masters directory.

Finally, the file contains the executable SeComp program command line shown next with its default settings:

```
cd ${SECOMPPATH}
./secomp -d ${SECOMPPATH}/secomp -r ${REPPATH}/secomp/reports -m
${MASTPATH}/secomp/masters
```

The line break in the previous example of the command line is not represented in the `~/secomp/run_secomp` file. It is a function of the word processing system used to produce this document.

The assignments in the `/secomp/run_secomp` file may be established in a `run_secomp` file set up on a client, however, it is vital that the `SECOMPPATH` variable be the same for all clients being served in a domain unless a client is prepared to run in a standalone configuration. This would require that the entire SeComp hierarchy be installed on that client. The other variables may be changed provided they make sense to the clients file system configuration.

3.5.5.5 ~/secomp/.secomp_paths

The `~/secomp/.secomp_paths` will be [re-]created at each execution of the SeComp tool. This file will contain path information used by the internal SeComp software. Do not modify this file. If problem exists where it is unknown where the SeComp tool is sourced or where its report files are being deposited, a quick glance at this file will provide that information.

3.5.6 SeComp Server Automount Configuration

The SeComp configurations depend on the correct automount configuration on the clients and correct exporting of the SeComp hierarchy on the server for the clients.

The server's NFS file share control file is configured to export the SeComp hierarchy. The following entry will be entered as a part of the default configuration (the example assumes a Solaris platform configuration):

```
share -F nfs -o rw=allowed anon=0 /etc/secomp
```

3.5.7 SeComp Client Configurations

Each client that executes SeComp in the client-server environment must be configured to understand its environment. Each client must at least be configured with the automount information that identifies the location of the SeComp server. The remaining configuration items such as the runtime, reports, and masters directories will be configured with the defaults shown in the SeComp Server Configuration section. These may be used as they are, and as discussed previously, it is recommended that the defaults be used for most SeComp operations.

A workstation running SeComp in standalone mode may not require any configuration if the default configuration satisfies the needs of the enterprise. The SeComp tool will figure out that it is running on a non-networked workstation and configures itself accordingly.

3.5.8 SeComp Clients in Client-Server Mode

The SeComp client will be configured to know where the SeComp runtime directories are by modifying the `/etc/auto_master` file, shown next with the default settings (the examples assume a Solaris platform):

```
/-      /etc/auto_direct
```

This points to the file `/etc/auto_direct` which contains the server location information, shown next with the default settings:

```
/etc/secomp  [server_name]:/etc/secomp
```

where *server_name* will be replaced with the correct SeComp server name for the enterprise.

3.6 Modifying run_secomp

The client may specify where the SeComp repository directories may be located. If the client does not specify this, the SeComp will default to the `/etc` locations that are recommended for use. For example, if a client were required to reference a special set of master files, another `run_secomp` file could be set on the client and referenced in the cron entry. If the client were to specify the location of the masters directory, the `run_secomp` file could be modified to cause this:

```
SECOMPPATH=/etc
REPPATH=/etc
MASTPATH=/usr

cd ${SECOMPPATH}
./secomp -d ${SECOMPPATH}/secomp -r ${REPPATH}/secomp/reports -m
${MASTPATH}/secomp/masters
```

Changing `MASTPATH` in this manner will cause a master file to be referenced in the `/usr/secomp/masters` directory on the client, unless, of course, the `/usr` directory is actually mounted from another system.

3.7 SeComp Reports

All SeComp reports will be stored in the `~/secomp/reports` directory unless the report directory location is modified by the enterprise. In the client-server mode, each client will cause the creation of a subdirectory under the reports directory named by the `uname -n` output for the client host. For example, in the default runtime configuration a host named *client1* would find its reports in:

```
/etc/secomp/reports/client1
```

Also, the reports directory will contain subdirectories that store the contents of the reports generated. The directory containing the latest reports run will be linked to the directory name *latest*. All of the report directories (except the linked directory *latest*) will be named by a time stamp reflecting the execution time.

The actual reports contained in the report subdirecties are named for the task it reports and will be suffixed by *.rpt,* for example, for the sysconfig task, a report named:

```
/etc/secomp/reports/client1/latest/sysconfig.rpt
```

would be generated for the client1 host.

If the password vulnerability check, cckpswd is run, there will be two additional files in the report subdirectory with the somewhat cryptic name of `[process_id].out`. The crack engine names the output files with the process ID of the crack process, this will replace the *process_id* portion of the name. For example, assume the process ID of the crack process is 8895. The crack engine will place the result of the process in a file called:

```
/etc/secomp/reports/client1/latest/8895.out
```

There may be more than one *.out* file that crack generates. The `view_rep` command discussed in the "SeComp Commands" section will automatically add the pertinent contents of the [*process_id*]`.out` files to the password checking report.

3.8 Installing SeComp from Tape

Installing Version 1.0 of the SeComp tool is accomplished via the following simple procedures outlined for the Solaris and Hp-UX OS's.

3.8.1 Solaris 2.5 Installation

The SeComp program will operate the same on all three Solaris platform OS's. Follow these steps to install:

1. Determine the Solaris server that will house the SeComp hierarchy.
2. Login to the server as root.
3. Insert the 8 millimeter tape into the tape drive.
4. Issue the following tar command at the command line:

```
$ cd /etc
$ tar xvf /dev/rmt/[device minor number]
```

The tar command will deposit a tar file named secomp.tar in the `/etc` directory.

5. Still in `/etc`, issue the following tar command:

$ tar xvf secomp.tar

The tar command will deposit the secomp directory hierarchy in the `/etc/secomp` directory. Installation is complete, proceed to Subsection 4.6 to configure the SeComp tool for use.

Please refer to the DII COE Security Compliance Tool Administrators Reference Manual for additional information.

4. UBDEV

This contains the developer's toolkit for Unified Build in a tar format. Please refer to the Unified Build 3.0 Application/TDA Toolkit Application Programmers Interface (API) Manual for information on API's and man pages.